UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,610	10/27/2003	William Eric Hall	YOR920030534US1(8728-664)	5733

22150 7590 06/06/2007

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/694,610	HALL ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 26.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, Applicant asserts Hawkes fails to teach (a) obtainng "a corresponding plurality of Ciphertext blocks" and obtaining "a Ciphertext checksum responsive to each of the corresponding plurality of Ciphertext blocks" and (b) Hawkes fails to teach a plaintext checksum and a ciphertext checksum are generated from the same block or element. Examiner respectfully disagrees because Hawkes teaches outputting a first checksum from a set of specified plaintext blocks (i.e. a plurality of plaintext blocks) and outputting the second checksum from a set of specified ciphertext blocks (i.e. a plurality of ciphertext blocks); where any specified ciphertext blocks evidently does not exclude the same set of specified plaintext blocks that generates the first checksum.

Claim Objections

4. Claim 26 is objected to because of the following informalities: "the partial ciphertext" should be replaced with "a partial ciphertex". Appropriate correction(s) is (are) required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 25 and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 25 and 26 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements regarding what to do with the obtained "partial ciphertext" in order to produce a useful result with practical usage in the real world (as a patentable feature). See MPEP § 2172.01 and MPEP §7.05.01.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 – 9, 11 – 21, 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (U.S. Patent 2005/0074116), here after referred to as "AAP", in view of Hawkes et al. (U.S. Patent 2004/0017913).

As per claim 1, 13 and 24, AAP teaches a method for generating a simple universal hash value, the method comprising:

inputting a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a corresponding plurality of Ciphertext blocks (AAP: Para [0021] – [0022] and Figure 2).

However, AAP does not teach combining the Plaintext checksum and the Ciphertext checksum to obtain the simple universal hash value:

Hawkes teaches:

combining the Plaintext checksum and the Ciphertext checksum to obtain the simple universal hash value (Hawkes : Page 11, Right Column, Last line – Page 12 Line 1 –2: (a) the authentication tag is qualified to be used as the simple universal hash value for content authentication purpose in a form of checksum or hash value (b) the 1st and 2nd checksum can be obviously referred to as an equivalent form of the plaintext checksum and the ciphertext checksum respectively);

computing a Plaintext checksum value responsive to each of the plurality of Plaintext blocks (Hawkes : Page 11, Right Column, Last 7th – 8th Line: a checksum from a set of specified plaintext blocks, as taught by Hawkes);

processing the plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum responsive to each of the corresponding plurality of ciphertext blocks (Hawkes : Page 1, Para [0012] Line 27 – 28 and Para [0077] and Page 11, Right Column, Last 7th – 8th Line: a checksum can be derived from a set of text data blocks with a encrypting key; where the text data block can be either a set of cipher text blocks

or a set of plaintext blocks that may be interchangeably accommodated as necessary that can be obviously recognized by an ordinary skill in the art, as taught by Hawkes).

As per claim 2 and 14, AAP as modified teaches the Plaintext checksum, the Ciphertext checksum and the universal hash value are all of the same size (Hawkes : Page 1, Para [0012] Line 1 – 6).

As per claim 3 and 15, AAP as modified teaches the size of the first of the plurality of Plaintext blocks is a multiple of the size of the universal hash value (Hawkes: Para [0039] and Page 1, Para [0012] Line 1 – 6).

As per claim 4 and 16, AAP as modified teaches computing a partial sum by taking the exclusive-or sum of the plurality of Plaintext blocks and reducing the partial sum to obtain the Plaintext checksum (Hawkes: Para [0057]: XOR would reduce the size of checksum).

As per claim 5 and 17, AAP as modified teaches reducing the partial sum comprises computation of the exclusive-or sum of equal sized segments of the partial sum (Hawkes: Para [0057], Para [0071] and Page 1, Para [0012] Line 1 – 6).

As per claim 6 and 18, AAP as modified teaches reducing the plurality of Plaintext blocks to obtain a plurality of partial Plaintext blocks; and combining the

plurality of partial Plaintext blocks using an exclusive-or sum to obtain the Plaintext checksum (Hawkes: Para [0057], Para [0071] and Para [0012]).

As per claim 7 and 19, AAP as modified teaches reducing the plurality of Plaintext blocks comprises the computation of the exclusive-or sum of equal sized segments of the Plaintext blocks (Hawkes: Para [0057], Para [0071] and Para [0012]).

As per claim 8 and 20, AAP as modified teaches selecting partial Ciphertexts using the third key from each of the plurality of Ciphertext blocks; and combining the partial Ciphertexts using an exclusive-or sum to obtain the Ciphertext checksum (Hawkes: Para [0057], Para [0071] and Page 1, Para [0012] Line 27 – 28 and Para [0077]: a checksum can be derived from a set of text data blocks with a encrypting key; where the text data block can be either a set of cipher text blocks or a set of plaintext blocks that may be interchangeably accommodated as necessary that can be obviously recognized by an ordinary skill in the art, as taught by Hawkes).

As per claim 9 and 21, AAP as modified teaches selecting partial Ciphertexts using the third key from a Ciphertext block comprises the process of using the bits of the third key as an index into the Ciphertext block (AAP: Para [0022] Last Line).

As per claim 11 and 23, AAP as modified teaches the Plaintext checksum and the Ciphertext checksum are combined by an exclusive-or operation to obtain the

universal hash value (Hawkes: Para [0057], Para [0071], Para [0012] Page 11, Right Column, Last line – Page 12 Line 1 –2: (a) the authentication tag is qualified to be used as the simple universal hash value for content authentication purpose in a form of checksum or hash value (b) the 1st and 2nd checksum can be obviously referred to as an equivalent form of the plaintext checksum and the ciphertext checksum respectively).

As per claim 12, AAP as modified teaches obtaining partial checksums using known universal hash functions from the third key and each of the plurality of Ciphertext blocks; and combining the partial checksums using an exclusive-or sum to obtain the Ciphertext checksum (Hawkes: Para [0057], Para [0071] and Para [0012).

Allowable Subject Matter

7. Claim 10 and 22 are objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. Claims 25 – 26 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100